UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Seizure of *(Briefly describe the property to be seized)* Cryptocurrency, virtual currency, and other things of value stored in or accessible at nine cryptocurrency wallet addresses	)	Case No. 5:24-MJ-1976-BM

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of North Carolina is subject to forfeiture to the United States of America under 18 U.S.C. § 981 *(describe the property:)*

See Attachment A hereto for property description.

The application is based on these facts:

Please see the facts set forth in the attached affidavit.

☑ Continued on the attached sheet.

Applicant's signature

David Harding, Special Agent, FBI
Printed name and title

On this day, Special Agent David Harding appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Application for a Warrant to Seize Property Subject to Forfeiture. via telephone at 5:01 pm.

Date: July 21, 2024

Judge's signature

City and state: Raleigh, North Carolina

BRIAN S. MEYERS, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEIZURE WARRANTS

I, Federal Bureau of Investigation Special Agent David Harding, hereby depose and state as follows:

INTRODUCTION

1. I submit this affidavit in support of an application for the issuance of a seizure warrant for the funds located in nine cryptocurrency wallet addresses (collectively, "**the Subject USDT Addresses**"), to wit:

a. All Tether ("USDT") held in a wallet address identified by 0xF6438DeD9Eb47AAB9d41664664F201B498f905D6 (hereinafter "USDT Address A");

b. All USDT held in a wallet address identified by 0x6275Ca02c006E843b11FF9ea3c4d2a051a170e61 (hereinafter "USDT Address B");

c. All USDT held in a wallet address identified by 0x8b10c643D42374D63824a39932c3e66c5f07E3F4 (hereinafter "USDT Address C");

d. All USDT held in a wallet address identified by 0xc48436c1674EFcFe8fb8E96c3F6504324dD6D50e (hereinafter "USDT Address D");

e. All USDT held in a wallet address identified by 0x1291bF41339300ebDBB4B289143b6d5f373ab553 (hereinafter "USDT Address E");

f. All USDT held in a wallet address identified by 0x06Ecb24C52C2d606d4F52ba9B7987002f0915CDc (hereinafter "USDT Address F");

g. All USDT held in a wallet address identified by 0x87407128829036l738Ea12Cd1389f4bcB4875eF3 (hereinafter "USDT Address G");

h. All USDT held in a wallet address identified by 0xD9B56f584EE14eA1Bc8712D0335fbb63E26AE693 (hereinafter "USDT Address H"); and

i. All USDT held in a wallet address identified by 0xDc35cE037722e2196a8B3eB9da64648Bc0E037C8 (hereinafter "USDT Address I");

2. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that unknown subjects have violated Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud) and laundered the proceeds of that activity in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) (money laundering and conspiracy to commit money laundering). There is also probable cause to believe that the **Subject USDT Addresses** received the proceeds of the wire fraud scheme described below and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C). Moreover, as indicated below, there is also probable cause to believe the **Subject USDT Addresses** are involved in money laundering transactions and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A). Accordingly, I request that the Court authorize the attached warrant for seizure of the assets described herein.

3. This Affidavit is intended to show only that there is sufficient probable cause for the requested forfeiture seizure warrants described more fully below and does not set forth all of my knowledge about this matter. The information contained herein comes from my personal knowledge; information conveyed by law enforcement officers and cryptocurrency exchange representatives; and publicly available information.

AFFIANT BACKGROUND AND EXPERTISE

4. I am a Special Agent with the Federal Bureau of Investigation assigned to the Charlotte, North Carolina Field Office with duty in the Raleigh Resident Agency. I have been employed as a Special Agent with the FBI since 2012 and worked a variety of federal criminal investigations, including but not limited to complex financial crimes.

APPLICABLE AUTHORITY

5. CRIMINAL STATUTES

a. Title 18, United States Code, Section 1343, makes it a crime to knowingly execute, or attempt to execute, a scheme or artifice to (1) obtain money or property by means of false or fraudulent pretenses, representations, or promises; (2) that are material; (3) with the intent to defraud; and (4) where the defendant used, or caused to be used, a wire communication to carry out or attempt to carry out an essential part of the scheme.

b. Title 18, United States Code, Section 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction involving the proceeds of specified unlawful activity knowing that the transaction is designed, in whole or in part, to conceal or disguise the nature, location, source, ownership, or control of those proceeds. Wire fraud activity conducted in violation of Title 18, United States Code, Section 1343 is a specified unlawful activity pursuant to Title 18, United States Code, Section 1956(c)(7), per its cross reference to Title 18, United States Code, Section 1961(1).

6. SEIZURE AND FORFEITURE STATUTES

a. **Wire fraud forfeiture:** Title 18, United States Code, Section 981(a)(1)(C) provides for the civil forfeiture of "[a]ny property, real or personal, which constitutes or is derived from

proceeds traceable" to the violation of an enumerated statute constituting a specified unlawful activity. Specified unlawful activities are detailed therein, as well as at Title 18, United States Code, Sections 1956(c)(7) and 1961(1), which enumerates Title 18, United States Code, Section 1343 as a specified unlawful activity.

b. **Money laundering forfeiture**: Title 18, United States Code, Section 981(a)(1)(A) provides for the civil forfeiture of any property, real or personal, that is involved in a transaction or attempted transaction in violation Title 18, United States Code, Sections 1956, 1957, or 1960.

c. **Seizure warrant authority:** Title 18, United States Code, Sections 981(b)(2) and (3) provide that seizures executed for purposes of civil forfeiture shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure. Moreover, seizure warrants may be issued in any district in which a forfeiture action may be filed and may be executed in any district in which the property is found. Federal Rule of Criminal Procedure 41 governs the issuance of criminal search and seizure warrants.

d. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains, and to divest criminal actors from the apparatus allowing them to engage in criminal activity. *See United States v. Newman*, 659 F.3d 1235, 1242 (9th Cir. 2011); *United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006). To that end, in cases involving a money laundering offense, the forfeiture statutes connected to money laundering offenses permit the government to forfeit property "involved in" money laundering. Such property includes "untainted property" commingled with "tainted" property, when that untainted property is used to facilitate the laundering offense, such as by obscuring the nature, source, location, or control of any criminally derived property. *See* Title 18, United States Code, Sections 981(a)(1)(A), 982(a)(1); *see also United*

States v. Kivanc, 714 F.3d 782, 794-95 (4th Cir. 2013); *United States v. Huber*, 404 F.3d 1047, 1056-1058 (8th Cir. 2005).

e. Based on my training, experience, and the information contained in this affidavit, there is probable cause to believe that funds in the **Subject USDT Addresses** are subject to seizure and civil forfeiture as proceeds traceable to a wire fraud scheme. The balances of the **Subject USDT Addresses** are also subject to seizure and civil forfeiture as property involved in money laundering transactions.

BACKGROUND OF CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. *Cryptocurrency and Blockchain Generally*: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Tether, USD Coin, and DAI. Each unit of cryptocurrency is often referred to as a "coin" or "token." In general, most cryptocurrencies are considered fungible assets. For example, Bitcoin is considered fungible because each unit of Bitcoin is equivalent to any other unit, meaning they have the same quality and functionality. Regardless of when a unit of Bitcoin was issued ("mined"), all Bitcoin units are part of the same blockchain and have the same functionality. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in cryptocurrency,

whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[1] Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets.

b. *Wallets*: Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can be either "custodial" or "non-custodial" (also referred to as "centralized/decentralized" or "hosted/non-hosted"). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet's private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a

[1] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

cryptocurrency exchange, and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.

c. *Exchanges/Exchangers*: Virtual currency "exchangers" and "exchanges" (also referred to as a "Virtual Asset Service Provider" [VASP]), such as Binance, Coinbase, Kraken, and Crypto.com, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies.

d. *Centralized/Decentralized Exchanges*: Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges consist of peer-to-peer marketplaces where users can trade cryptocurrencies in a non-custodial manner, without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or "swap", one type of cryptocurrency for another, for which the user pays a transaction fee. Centralized exchanges that conduct business in the United States are required to verify their customers' identities and abide by Know-Your-Customer/Anti-Money Laundering (KYC/AML) regulations.

e. *Tether*: Tether, widely known as "USDT," is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a "stablecoin." USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is connected to Bitfinex, a cryptocurrency exchange registered in the British Virgin Islands.

f. USDT is hosted on the Ethereum and Bitcoin blockchains, among others. Ethereum ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a

platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

g. Like other virtual currencies, USDT is sent to and received from USDT "addresses." A USDT address is somewhat analogous to a bank account number and is represented as a 26-to 35-character-long case-sensitive string of letters and numbers. Users can operate multiple USDT addresses at any given time, with the possibility of using a unique USDT address for every transaction. Although the identity of a USDT address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular USDT address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. Unlike Bitcoin, one of the most popular cryptocurrencies in use today, USDT is "centralized", meaning that it is issued and controlled by a governing body. Most other cryptocurrencies are "decentralized" and have no such governing body.

FACTS SUPPORTING PROBABLE CAUSE

THE SCHEME

8. This case concerns a cryptocurrency investment fraud scam perpetrated on victims throughout the United States, including in the Eastern District of North Carolina. The scheme often begins when a fraudster sends a victim a seemingly innocuous and misdialed text message, or through sending an unsolicited message to a victim's social media account. From there, the fraudster will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

9. Once the fraudster has established a trusted relationship with the victim, the fraudster brings the victim into a cryptocurrency investment scheme. This fraudster typically claims to have a technique to quickly make large profits, either through personal expertise with cryptocurrency, or through a trusted relative or friend with insider information. The investment schemes have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns. The investment platforms are a ruse, and the funds contributed are routed directly to a cryptocurrency address the fraudsters control. In reality, the victims do not have actual "accounts" at the fake companies – as soon as the victim sends cryptocurrency to the deposit address provided by the fraudsters, it is immediately moved through many other wallets in order to launder the funds and make them harder to trace. The victims are able to see what they believe are their deposits on the

fraudulent website, and the purported large returns on their investments are designed to convince them to invest more.

10. When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses, such as being told they are required to pay "taxes" or "penalties" in order to release their funds. The "tax" payments are an attempt by the scammers to elicit even more money out of the victims. The fraudsters, in the form of "customer service" for the fraudulent website, will continue to ask for additional payments from the victim, and will not release the funds regardless of how much is paid.

11. In this case, multiple victims, one of whom (hereinafter "K.W.") resides in the Eastern District of North Carolina, were victims of a cryptocurrency investment fraud scheme. This affidavit discusses two victims ("K.W." and "J.B.") of the same organization perpetrating the same investment fraud scheme. The victims were approached and recruited through the guise of a romantic relationship in order to develop a trusted relationship. Once the romantic relationship was established, the fraudster introduced K.W./J.B. to the fictitious trading platform, Bitkanant (the name of this trading platform is similar to a legitimate cryptocurrency trading platform, Bitkan). Based on an analysis of the fake investment platforms that all the victims were directed to, as well as tracing of the cryptocurrency that the victims sent, agents believe that the victims were all likely victimized by the same person or group. The following sections detail the background of one victim's enticement into the scheme. This is followed by a section which demonstrates the link between the victims and shows that there are likely to be many more additional victims of the same group.

Victim K.W.

12. K.W. is 67 years old and a resident of Angier, North Carolina. In January 2023, a person claiming to be a woman named "Jeanie" contacted K.W. via text message and they began exchanging messages not related to investing or cryptocurrency. They later communicated via WhatsApp and Telegram. Jeanie (who later said her real name was Li Xueli) said she worked in fashion design in Miami, Florida. Jeanie also claimed to be from Hong Kong, with her mother being Chinese and her father being English. Jeanie provided multiple pictures of herself, some of which were later found associated with different names on various social media and websites, such as LinkedIn. There are even screenshots of text communications with her picture attempting to engage other individuals.

13. Eventually the conversation turned to finances and investing. Jeanie claimed her uncle lived in Chicago, and he and his team developed an algorithm predicting the up-and-down price movement of Bitcoin and Ethereum on particular days at particular times. Jeanie then introduced K.W. to Bitkan, the legitimate international cryptocurrency exchange platform. But Jeanie provided K.W. the website link, Bitkanant.com/h5#/home, which was not the link to Bitkan, but instead the link to a fake cryptocurrency trading platform.

14. In or around the end of January 2023, after receiving assurances about the safety of the website for investments and the trust K.W. had developed for Jeanie due to their romantic relationship, K.W. agreed to create an account on Bitkanant.com/h5#/home and make some small investments. In total, K.W. invested approximately $95,000. K.W. transferred money to his cryptocurrency wallets at Cypto.com or Coinbase and then transferred either Bitcoin or Ethereum to what K.W. believed were his wallets at Bitkan. K.W. made some trades on the website based on Jeanie's recommendation from "her uncle" and made significant profits in a short period of time. K.W. was then able to make small

withdrawals from what K.W. believed was his Bitkan account. This gave K.W. further comfort in the platform and convinced K.W. to make additional investments. Between February and March 2023, Jeanie manipulated K.W. into investing his entire individual retirement account (IRA), totaling approximately $1.8 million.

15. When K.W. attempted to withdraw any funds over $50,000, he received a message that the withdrawal was disallowed unless taxes, fines, and fees were transferred to the website as USDT. K.W. transferred approximately $669,000, which included a 20% tax, approximately $516,000 due to a trigger in the system claiming money laundering, $140,000 for a 5-year VIP pass, $100,000 for a blockchain large transfer channel, $57,000 to return profit the site claimed was an irregular operation, and $100,000 for an instant withdrawal fee. In total, the purported "taxes, fines, and fees" transferred by K.W. amounted to $1.6 million.

16. In or around April 2023, Jeanie began having less communication with K.W. The last contact was in July 2023. Soon after communication with Jeanie ended, Bitkanant.com/h5#/home was taken down. In or around August 2023, K.W. located a new website on his own, Bitkancie.com, which was the same exact site as Bitkanant.com/h5#/home and K.W. was even able to log in using the same credentials and see his investments. K.W. subsequently reported the fraud to the FBI Internet Crime Complaint Center on August 3, 2023, leading to the initiation of this investigation.

Tracing of Victim K.W.'s Funds to the **Subject USDT Addresses**

17. Seven of K.W.'s cryptocurrency transactions were traced to the **Subject USDT Addresses**, as detailed below. The traces were conducted using the Last-In-First-Out accounting principle – meaning the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

18. The following two transactions made by K.W. were traced to **USDT Address A**:

a. On February 4, 2023, K.W. sent 199,990 USDT from K.W.'s Crypto.com account to address 0x96C93A, which K.W. believed to be with Bitkan. From there, 199,990 USDT was sent to 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address A on March 11, 2023, as part of a 500,000 USDT transaction.

b. On February 6, 2024, K.W. sent 87,990 USDT from K.W.'s Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. From there, 87,990 USDT sent to 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address A on March 11, 2023, as part of a 500,000 USDT transaction.

c. As of May 8, 2024, when the address was frozen by Tether at FBI request, approximately 499,535 USDT was present in USDT Address A, 287,980 of which can be traced as proceeds directly from K.W.

19. The following transaction made by K.W. was traced to **USDT Address B**:

a. On March 8, 2023, K.W. sent 199,990 USDT from K.W.'s Crypto.com account to address 0x96C93A, which K.W. believed to be with Bitkan. From there, 199,990 USDT was sent to 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address B in eleven installments from March 11, 2023 to March 21,2023 totaling 243,099 USDT.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 684,279 USDT was present in USDT Address B, 151,708 of which can be traced as proceeds directly from K.W.

20. The following transaction made by K.W. was traced to **USDT Address C**:

a. On April 21, 2023, K.W. sent 199,990 USDT from his Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address C on May 11, 2023 as part of a 500,000 USDT transaction.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,000 USDT was present in USDT Address C, 199,990 of which can be traced as proceeds directly from K.W.

21. The following transaction made by K.W. was traced to **USDT Address D**:

a. On April 22, 2023, K.W. sent approximately 108,141 USDT from his Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address D on May 11, 2023 as part of a 500,000 USDT transaction.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,004 USDT was present in USDT Address D, 108,141 of which can be traced as proceeds directly from K.W.

22. The following two transaction made by K.W. were traced to **USDT Addresses E**:

a. On March 9, 2023, K.W. sent 180,790 USDT from his Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address E on March 11, 2023 as part of a 500,000 USDT transaction.

b. Also on March 9, 2023, K.W. sent approximately 126.61 ETH from his Coinbase account to address 0x96C93A which K.W. believed to be with Bitkan. The 126.61 ETH was transferred to address 0x7C9702 and converted to 193,745 USDT, using the decentralized exchange Tokenlon. The majority of these funds were transferred to several more addresses, commingled with additional USDT, and ultimately sent to USDT Address E on March 11,2023 as part of a 500,000 USDT transaction.

c. As of May 8, 2024, when the address was frozen by Tether at FBI request, approximately 499,424 USDT was present in USDT Address E, 294,044 of which can be traced as proceeds directly from K.W.

23. In tracing K.W.'s cryptocurrency transactions, agents determined that two addresses (**USDT Address H** and **USDT Address I**) had funds remaining after the pass-through transfer of K.W.'s funds. Through the analysis described below, Addresses H and I were used for the purposes of commingling the proceeds of the fraud with other USDT[2] in furtherance of laundering the proceeds. Specifically:

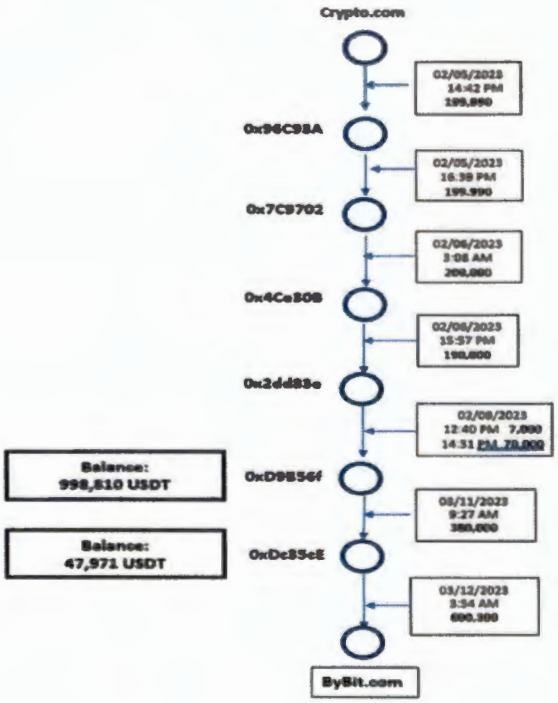
a. On February 5, 2023, K.W. sent approximately 199,990 USDT from his Crypto.com account to address 0x96C93A, which K.W. believed to be with Bitkan. These funds were

[2] Analysis of the addresses H & I indicates other deposits into the address were also fraudulent proceeds.

commingled with additional USDT, transferred through several more addresses, including USDT Address H (0xD9B56f) and USDT Address I (0xDc35cE), and ultimately sent to an address at the exchange Bybit.com on March 12, 2023 as part of a 600,300 USDT transaction.

b. As of May 8, 2024, when the address was frozen by Tether at FBI request, approximately 998,810 USDT was present in USDT Address H, and 47,971 USDT was present in USDT Address I.

c. The following is a graphical representation of these transactions:



Victim J.B.

24. J.B. is an 83-year-old resident of Bayfield, Minnesota. In February 2023 a person claiming to be a woman named Alice contacted J.B. via text message, said she received his phone number from

another person, and that she wanted to verify it was really them. They later communicated via WhatsApp and Telegram. Alice (who later said her real name was Jengyi Lee) said she worked in fashion design in Miami, Florida. Alice also claimed to be from Hong Kong. J.B. and Alice eventually discussed cryptocurrency. J.B. said he had lost money on his investment in BTC and ETH, but he still held various cryptocurrencies in Coinbase. Alice introduced J.B. to what J.B. believed was a cryptocurrency trading platform called Bitkan. However, Alice deceived him into creating an account at a fraudulent site, Bitkanant, by providing the website address as "Bitkanant.com/h5#/home" rather than the true website address, Bitkan.com. Screenshots included below demonstrate how Alice deceived J.B. into accessing the fraudulent website rather than the legitimate Bitkan website.

25. In or around the middle of February 2023, J.B. transferred money to his wallets at Coinbase and then transfer either USDT or ETH to what J.B. believed were his wallets at Bitkan. J.B. made some trades on the website based on Alice's recommendation from her uncle and, according to Bitkan, made significant profit in a short period of time. Between February and April 2023, Alice manipulated J.B. into investing all of his savings, including a surrendered life insurance policy, totaling approximately $950,000.

26. In or around May 30, 2023, after Adult Protective Services was contacted by J.B.'s bank, the Bayfield County Sheriff's Office filed a fraud report to the FBI Internet Crime Complaint Center (IC3) on J.B.'s behalf. J.B. and the Bayfield County Sheriff's Office attempted to withdraw money from J.B.'s Bitkan account but were unsuccessful.

Tracing of Victim J.B.'s Funds to the **Subject USDT Addresses**

27. Two of J.B.'s cryptocurrency transactions were traced to the **Subject USDT Addresses**, as detailed below. The traces were conducted using the Last-In-First-Out accounting principle – meaning the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

28. The following transaction made by J.B. was traced to **USDT Address F**:

a. On March 9, 2023, J.B. sent 13.59 BTC from J.B.'s Coinbase.com account to address 3HvFNTok which J.B. believed to be with Bitkan. From there, the funds were converted to 268,865 USDT via Tokenlon and deposited at address 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address F on May 11, 2023, as part of a 500,000 USDT transaction.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,004 USDT was present in USDT Address F, 268,865 of which can be traced as proceeds directly from J.B.

29. The following transaction made by J.B. was traced to **USDT Address G**:

c. On April 14, 2023, J.B. sent 9.02 BTC from J.B.'s Coinbase.com account to address 07x788EB which J.B. believed to be with Bitkan. From there, the funds were converted to 18,896.26 USDT via Tokenlon and deposited at address 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address G on May 11,2023 as part of a 500,000 USDT transaction.

d. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,004 USDT was present in USDT Address G, 18,896.26 of which can be traced as proceeds directly from J.B.

Tracing of Other Probable Victims' Funds to the **Subject USDT Addresses**

30. There are several factors which indicate that the two victims described above are part of the same larger fraud scheme. These factors show that the **Subject USDT Addresses** have been used not only to launder the proceeds of criminal activity received from K.W. and J.B., but from numerous other victims who are unknown at this time.

a. *Shared cryptocurrency addresses and patterns of activity:* In cryptocurrency investment fraud schemes, victims are often given individual "burner" cryptocurrency addresses which are provided only to that particular victim. When a victim sends cryptocurrency to the burner address, the cryptocurrency is then quickly sent to another address where funds from multiple victims

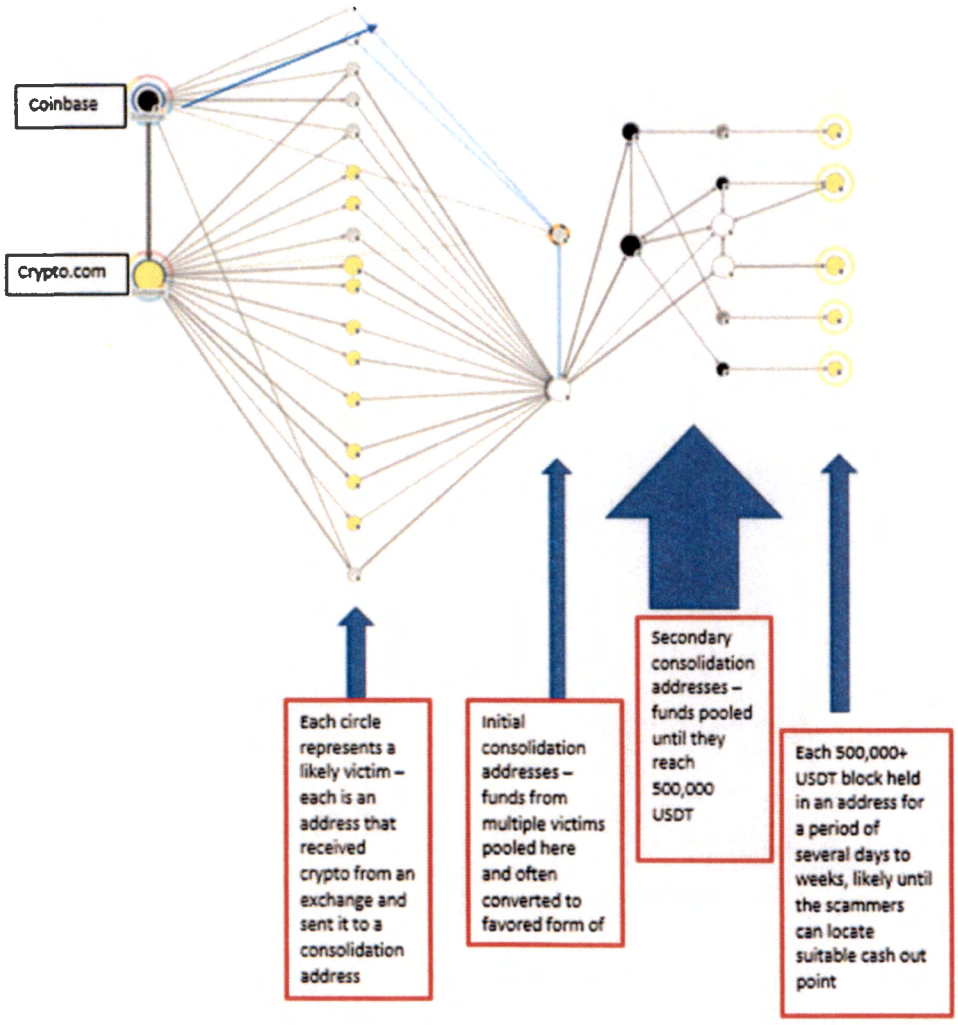
are consolidated. There are often multiple layers of consolidation addresses, which can be seen in this case. Specifically:

i. The tracing of victim transactions in this case showed that all of the transactions which led to Subject Addresses A, B, C, D, and E were sent through consolidation addresses, 0x96C93A and 0x7C9702. Transactions which led to USDT Address F and USDT Address G were sent through other addresses before passing through consolidation address 0x7C9702. USDT Address E and USDT Address F also shared consolidation address 0x02b725, and USDT Address C and USDT Address F shared consolidation address 0x1345ef.

ii. In sum, based on my training, experience, and the investigation to date, I believe that each victim transaction shows a common pattern of moving to an initial consolidation address, where it is converted to what appears to be the scammers' favored form of cryptocurrency, USDT. The USDT is then sent to a secondary consolidation address, where it is further comingled or transferred to several more addresses, then parceled out into addresses often containing approximately 500,000 USDT each. This was the common pattern for the transactions conducted on funds originating from K.W. and J.B.

b. The chart below was created by "backtracing" from the consolidation addresses that had been identified when tracing K.W. and J.B.'s transactions. In backtracing, instead of tracing forward to find out where the funds were sent, transactions were traced backward to see what other addresses had sent funds to the consolidation addresses, and where those funds originated from, which

in every case was an exchange. In my experience this technique is very successful in locating additional victims who may not have reported the scam or may not yet be aware they are a victim.



c. *Other Victim Reporting*: A search of the FBI's IC3 identified 71 other potential victims of this scam. These victims were located by searching for and "Bitturk" and "Bitkan" in the database. Each of these victims reported a similar scam to those detailed here, with some variations in how they

were recruited for the scam, the name the scammer used when contacting the victim, and the specific URL used to access the platform.

CONCLUSION

31. Based on information derived from the foregoing investigation, there is probable cause to conclude that the **Subject USDT Addresses** received and contain the proceeds of a wire fraud scheme in violation of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud). Those proceeds are subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C). In addition, there is probable cause to believe that the contents of the **Subject USDT Addresses** constitute property involved in money laundering transactions in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) (money laundering and conspiracy to commit money laundering), and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A). Accordingly, I respectfully request that warrants be issued authorizing the seizure of all funds in the **Subject USDT Addresses**.

SEIZURE PROCEDURE FOR THE SUBJECT USDT ADDRESSES

32. Should this seizure warrant be granted, law enforcement intends to work with Tether to seize the funds associated with the **Subject USDT Addresses**. In sum, the accompanying warrant would be transmitted to Tether, at which time Tether would "burn" (*i.e.*, destroy) the addresses at issue (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated with the **Subject USDT Addresses** and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of all forfeiture proceedings, to ensure that access

to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

Further your affiant sayeth naught.

David Harding
Special Agent
Federal Bureau of Investigation

On this 21st day of July, 2024, Special Agent David Harding appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit and telephone at 5:01 pm.

BRIAN S. MEYERS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency wallet. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

Nine cryptocurrency wallet addresses, to wit:

a. 0xF6438DeD9Eb47AAB9d41664664F201B498f905D6

b. 0x6275Ca02c006E843b11FF9ea3c4d2a051a170e61

c. 0x8b10c643D42374D63824a39932c3e66c5f07E3F4

d. 0xc48436c1674EFcFe8fb8E96c3F6504324dD6D50e

e. 0x1291bF41339300ebDBB4B289143b6d5f373ab553

f. 0x06Ecb24C52C2d606d4F52ba9B7987002f0915CDc

g. 0x874071288290361738Ea12Cd1389f4bcB4875eF3

h. 0xD9B56f584EE14eA1Bc8712D0335fbb63E26AE693

i. 0xDc35cE037722e2196a8B3eB9da64648Bc0E037C8